What is claimed is:

1. A system for automatically protecting private video content using cryptographic security for legacy systems, comprising:

a transportable storage medium, comprising:

recording logic intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

a frame buffer dividing the intercepted substantially continuous video signal into individual frames during recording, each individual frame storing a fixed amount of data in digital form, and combining decrypted frames into a substantially continuous video signal during playback; and

a processor encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames during recording and retrieving the encrypted frames and decrypting each encrypted frame using a decryption cryptographic key during playback; and

reading logic outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium.

2. A system according to Claim 1, further comprising:

an authentication module generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium, retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash.

3. A system according to Claim 2, further comprising:

an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

4. A system according to Claim 1, further comprising:

a validation module validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames.

5. A system according to Claim 1, further comprising:

an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

6. A system according to Claim 5, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

7. A system according to Claim 1, further comprising:

a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

8. A system according to Claim 1, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

9. A system according to Claim 8, further comprising:

a set of cryptographic instructions stored on the removable storage medium and employing at least one of the encryption cryptographic key and the decryption cryptographic key.

10. A method for automatically protecting private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

dividing the intercepted substantially continuous video signal into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption cryptographic key and storing the encrypted frames;

retrieving encrypted frames and decrypting each encrypted frame using a decryption cryptographic key;

combining the decrypted frames into a substantially continuous video signal; and

outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium.

11. A method according to Claim 10, further comprising:

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash; and

outputting the substantially continuous video signal upon successful comparison of the verification cryptographic hash and the original cryptographic hash.

12. A method according to Claim 11, further comprising:

providing an asymmetric cryptographic key pair comprising a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

13. A method according to Claim 10, further comprising:

validating the decryption cryptographic key against user-provided credentials prior to decrypting the encrypted frames.

14. A method according to Claim 10, further comprising:

providing an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

15. A method according to Claim 14, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

16. A method according to Claim 10, further comprising:

providing a symmetric cryptographic key pair comprising a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

17. A method according to Claim 10, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

18. A method according to Claim 17, further comprising:

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

19. A computer-readable storage medium holding code for performing the method according to Claims 10, 11, 12, 13, 14, 16, 17, or 18.

20. A system for encrypting private video content using cryptographic security for legacy systems, comprising:

recordation logic intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content;

a frame buffer dividing the signal into individual frames which each store a fixed amount of data in digital form;

a processor encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair and storing the encrypted frames on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair.

21. A system according to Claim 20, comprising:

the processor generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair, and storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair.

22. A system according to Claim 21, further comprising:

a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

23. A system according to Claim 20, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

24. A system according to Claim 20, further comprising:

a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

25. A system according to Claim 20, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

26. A method for encrypting private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content, and dividing the signal into individual frames which each store a fixed amount of data in digital form;

encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair; and

storing the encrypted frames on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair.

27. A method according to Claim 26, comprising:

encrypting each individual frame into encrypted video content using an encryption key selected from a cryptographic key pair;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair; and

storing the encrypted original cryptographic hash as a digital signature on the transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair.

28. A method according to Claim 27, further comprising:

employing a private key corresponding to the encryption cryptographic key and a public key corresponding to the decryption cryptographic key.

29. A method according to Claim 26, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

30. A method according to Claim 26, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

31. A method according to Claim 26, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

32. A computer-readable storage medium holding code for performing the method according to Claims 26, 27, 28, 29, 30, or 31.

33. A system for decrypting private video content using cryptographic security for legacy systems, comprising:

reading logic retrieving encrypted frames prior to playback from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair; and

a frame buffer combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form.

34. A system according to Claim 33, comprising:

the reading logic retrieving a digital signature included with the encrypted frames and encrypted using an encryption cryptographic key selected from a cryptographic key pair;

the processor generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash; and

the frame buffer combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage

medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash.

35. A system according to Claim 34, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

36. A system according to Claim 33, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

37. A system according to Claim 33, further comprising:

a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

38. A system according to Claim 33, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

39. A method for decrypting private video content using cryptographic security for legacy systems, comprising:

retrieving encrypted frames prior to playback from a transportable storage medium, the encrypted frames storing raw video content encrypted using an encryption cryptographic key selected from a cryptographic key pair;

decrypting each encrypted frame using a decryption cryptographic key selected from the cryptographic key pair; and

combining the decrypted frames into a substantially continuous video signal representing the raw video content in reconstructed form.

40. A method according to Claim 39, comprising:

retrieving a digital signature included with the encrypted frames and encrypted using an encryption cryptographic key selected from a cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash; and

combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash.

41. A method according to Claim 40, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

42. A method according to Claim 39, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

43. A method according to Claim 39, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

44. A method according to Claim 39, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

45. A computer-readable storage medium holding code for performing the method according to Claims 39, 40, 41, 42, 43 or 44.

46. A method for automatically authenticating private video content using cryptographic security for legacy systems, comprising:

a transportable storage medium, comprising:

recording logic intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

a frame buffer dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form and combining the individual frames into a substantially continuous video signal;

a processor generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key, storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium, retrieving the digital signature from the transportable storage medium, decrypting the encrypted original cryptographic hash using a decryption cryptographic key, generating a verification fixed-length cryptographic hash from at least one such individual frame, and comparing the verification cryptographic hash and the original cryptographic hash;

reading logic outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash.

47. A system according to Claim 46, further comprising:

an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

48. A system according to Claim 47, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

49. A system according to Claim 46, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

50. A system according to Claim 49, further comprising:

a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

51. A method for automatically authenticating private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal representing video content in the process of being recorded on a transportable storage medium;

dividing a substantially continuous video signal representing raw video content into individual frames which each store a fixed amount of data in digital form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium;

retrieving the digital signature from the transportable storage medium and decrypting the encrypted original cryptographic hash using a decryption cryptographic key;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash;

combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash.

52. A method according to Claim 51, further comprising:

providing an asymmetric cryptographic key pair comprising a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

53. A method according to Claim 52, wherein the asymmetric cryptographic key pair comprises at least one of an RSA-compatible key pair, a TwoFish-compatible key pair and a Diffie-Hellman-compatible key pair.

54. A method according to Claim 51, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

55. A method according to Claim 54, further comprising:

including a set of cryptographic instructions employing at least one of the encryption cryptographic key and the decryption cryptographic key on the removable storage medium.

56. A computer-readable storage medium holding code for performing the method according to Claims 51, 52, 54, or 55.

57. A system for digitally signing private video content using cryptographic security for legacy systems, comprising:

recordation logic intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content;

a frame buffer dividing the signal into individual frames which each store a fixed amount of data in digital form; and

a processor generating a fixed-length original cryptographic hash from at least one such individual frame, encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair, and storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair.

58. A system according to Claim 57, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

59. A system according to Claim 57, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

60. A system according to Claim 57, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

61. A method for digitally signing private video content using cryptographic security for legacy systems, comprising:

intercepting a substantially continuous video signal prior to recordation on a transportable storage medium, the signal representing raw video content;

dividing the signal into individual frames which each store a fixed amount of data in digital form;

generating a fixed-length original cryptographic hash from at least one such individual frame;

encrypting the original cryptographic hash using an encryption cryptographic key from a cryptographic key pair; and

storing the encrypted original cryptographic hash as a digital signature on a transportable storage medium for retrieval and decryption using a decryption key selected from the cryptographic key pair.

62. A method according to Claim 61, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

63. A method according to Claim 61, further comprising:

employing a substantially identical key corresponding to each of the encryption cryptographic key and the decryption cryptographic key.

64. A method according to Claim 61, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

65. A computer-readable storage medium holding code for performing the method according to Claims 61, 62, 63, or 64.

66. A system for verifying digitally signed private video content using cryptographic security for legacy systems, comprising:

reading logic retrieving frames prior to playback from a transportable storage medium, the frames storing raw video content and including a digital signature encrypted using an encryption cryptographic key selected from a cryptographic key pair;

a processor generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash; and

a frame buffer combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash.

67. A system according to Claim 66, further comprising:

a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

68. A system according to Claim 66, further comprising:

a removable storage medium storing at least one of the encryption cryptographic key and the decryption cryptographic key.

69. A method for verifying digitally signed private video content using cryptographic security for legacy systems, comprising:

retrieving frames prior to playback from a transportable storage medium, the frames storing raw video content and including a digital signature encrypted using an encryption cryptographic key selected from a cryptographic key pair;

generating a verification fixed-length cryptographic hash from at least one such individual frame and comparing the verification cryptographic hash and the original cryptographic hash; and

combining the individual frames into a substantially continuous video signal and outputting the substantially continuous video signal as video content in the process of being played from the transportable storage medium upon successful comparison of the verification cryptographic hash and the original cryptographic hash.

70. A method according to Claim 69, further comprising:

employing a public key corresponding to the encryption cryptographic key and a private key corresponding to the decryption cryptographic key.

71. A method according to Claim 69, further comprising:

providing at least one of the encryption cryptographic key and the decryption cryptographic key on a removable storage medium.

72. A computer-readable storage medium holding code for performing the method according to Claims 69, 70, or 71.